CHAPTER 1: Introduction

Coding Techniques

Francisco Valera Pintor

Departamento de INGENIERIA TELEMATICA
www.it.uc3m.es

TEACHERS

- Francisco Valera Pintor
- Mario Muñoz Organero
- Iván Vidal Fernández

LIST OF TOPICS

1. Introduction
2. Introduction to security
3. Symmetric-key cryptography
4. Public-key cryptography
5. Authentication & digital signatures
6. Applications

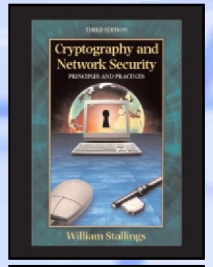
LABS

1. Linux/Windows passwords
2. Block cipher modes of operation: symmetric-key cryptography
3. PGP: public-key encryption

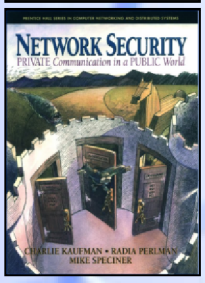
SCHEDULE

1. PRESENTATION (DAY 1)
   - 1.1 Course introduction
2. INTRODUCTION TO SECURITY (DAY 1)
   - 2.1 What is security
   - 2.2 Possible attacks and incidents
   - 2.3 Security services
     - 2.3.1 Confidentiality
     - 2.3.2 Integrity
     - 2.3.3 Authentication
     - 2.3.4 Non repudiation
     - 2.3.5 Access control
   - 2.4 Security mechanisms
     - 2.4.1 Naming and conventions
     - 2.4.2 Cryptosystems
   - 2.5 Ciphering location
     - 2.5.1 Hop by hop
     - 2.5.2 End to end
     - 2.5.3 End to end ciphering location
     - 2.5.4 Traffic analysis
3. SYMMETRIC ENCRYPTION
   - 3.1 Introduction (DAY 2)
     - 3.1.1 Model
     - 3.1.2 Cryptographic attacks
   - 3.2 Classic encryption techniques
     - 3.2.1 Substitution
       - 3.2.1.1 Cesar
       - 3.2.1.2 Simple
       - 3.2.1.3 Vignere
       - 3.2.1.4 Beaufort
     - 3.2.2 Transposition
     - 3.2.3 Evolutive keys
   - 3.3 Previous concepts
     - 3.3.1 Computational security
     - 3.3.2 Types of ciphers
   - 3.4 DES
     - 3.4.1 History
     - 3.4.2 Characteristics
     - 3.4.3 Properties
     - 3.4.4 Operation modes DAY 3
       - 3.4.4.1 ECB
       - 3.4.4.2 CBC
       - 3.4.4.3 CFB
       - 3.4.4.4 OFB
     - 3.4.5 Triple DES
       - 3.4.5.1 Double DES
       - 3.4.5.2 Triple DES
   - 3.5 Rijndael
     - 3.5.1 Introduction to AES
     - 3.5.2 Structure
   - 3.6 Key distribution
     - 3.6.1 Introduction
     - 3.6.2 Previous ideas
       - 3.6.2.1 Keys to distribute
       - 3.6.2.2 Update frequency
       - 3.6.2.3 Key generation
     - 3.6.3 Distribution techniques (DAY 4)
       - 3.6.3.1 Direct
       - 3.6.3.2 Indirect
       - 3.6.3.3 Distribution protocols
4. ASYMMETRIC ENCRYPTION (DAY 5)
   - 4.1 Introduction
   - 4.2 Mathematical basis
     - 4.2.1 Congruence
     - 4.2.2 Euclides Algorithm
     - 4.2.3 Euler function
     - 4.2.4 Modified Euclides algorithm
   - 4.3 RSA
     - 4.3.1 Introduction
     - 4.3.2 Number theory
     - 4.3.3 Examples
     - 4.3.4 Computational details
   - 4.4 ElGamal algorithm
   - 4.5 Elliptic curves (DAY 6)
     - 4.5.1 Curves theory
     - 4.5.2 Need of finite fields
     - 4.5.3 ElGamal algorithm
     - 4.5.4 Diffie-Hellman algorithm
5. AUTHENTICATION AND DIGITAL SIGN
   - 5.1 Problem
     - 5.1.1 Introduction
     - 5.1.2 Previous schemes
   - 5.2 Integrity
     - 5.2.1 Encryption +CRC
     - 5.2.2 Cryptographic Checksum
       - 5.2.2.1 Introduction
       - 5.2.2.2 Computational security
   - 5.3 Hash functions (DAY 7)
     - 5.3.1 Introduction
     - 5.3.2 Properties
     - 5.3.3 Hash function applications
       - 5.3.3.1 MICs
       - 5.3.3.2 Encryption
     - 5.3.4 Hash algorithms
       - 5.3.4.1 MAC and MDC
       - 5.3.4.2 Based on encryption blocks
       - 5.3.4.3 SHA
   - 5.4 Digital sign
     - 5.4.1 DS requirements
     - 5.4.2 DS algorithms
     - 5.4.3 Certification
       - 5.4.3.1 Introduction
       - 5.4.3.2 X.509
       - 5.4.3.3 Revocation
       - 5.4.3.4 Process description
       - 5.4.3.5 Digital sign algorithms
   - 5.5 Symmetric key distribution using asymmetric encryption (DAY 8)
     - 5.5.1 Asymmetric encryption
     - 5.5.2 Diffie-Hellman
6. APPLICATIONS
   - 6.1 Network layer security: IPSec

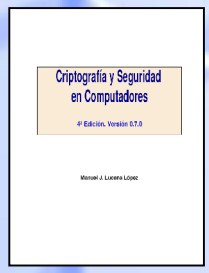
BIBLIOGRAPHY



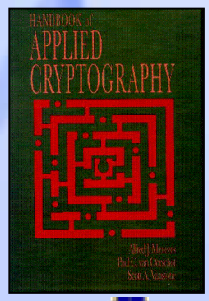
- ***Cryptography and network security. Principles and Practice***
  Fourth edition
  Williams Stallings. Prentice Hall. 2006



- ***Network security : private communication in a public world***
  C. Kaufman, R. Perlman, M. Speciner, E. Cliffs.
  Prentice Hall, 2002



- ***Criptografía y seguridad en computadores***
  Manuel José Lucena López. 2005.



- ***Handbook of applied cryptography***
  Alfred J. Menezes, Paul C. van Oorschot and
  Scott A. Vanstone.2001.